Amendments to the Specification:

Please replace the paragraphs at page 4, line 5 – page 5, line 2 with the following rewritten paragraphs:

A signature key is denoted by ~~(x, □, p)~~ (x, γ, p) and a verification key is denoted by ~~(y, □, p)~~, (y, γ, p) wherein p denotes a prime number ~~and □ denotes~~ and γ denotes a positive constant smaller than p. These integers are in relation represented by the equation (1)

[Equation 1]

(1) ~~y=□^{x}(mod p)~~ $y = \gamma^x \pmod{p}$

Calculation of the private integer x from the public integer y is a discrete logarithm problem, and it is difficult to get x by means of calculation if p is sufficiently large (500 bits or larger).

A prover generates a random number k which is mutually prime to p–1, and calculates a signature for a message m by use of the equations (2) and (3).

[Equation 2]

(2) ~~r=□^{k}(mod p)~~ $r = \gamma^k \pmod{p}$

[Equation 3]

(3) $s = (h(m) - xr)\, k^{-1} \pmod{p-1}$

wherein h denotes a one-way hash function. A prover sends the message m and signature (r, s) to a verification side.

The verifier receives m and (r, s), and checks whether the equation (4) holds.

[Equation 4]

(4) ~~□$^{h(m)}$ =y^{r}r^s(mod p)~~ $\gamma^{h(m)} = y^r r^s \pmod{p}$

If the equation holds, then it is proved that m is a message prepared by the prover.